REMARKS

Claims 1-28 and 30-35 are pending in this application. In the Office Action, the Examiner rejected claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35 under 35 U.S.C. 103 as being unpatentable over U.S. Patent 6,233, 565 to Lewis, et al. (Lewis) in view of U.S. Patent 6,976,162 to Ellison, et al. (Ellison), and further in view of U.S. Patent 5,604,805 to Brands. Claims 1-5, 12, 14-16, 18, 23, 24, 30 and 33 were rejected as being unpatentable under 35 USC 103 over Lewis, in view of U.S. Patent 5,850,442 to Muftic, and further in view of Ellison, and still further in view of Brands. In addition, each of pending claims 1-28 and 29-35 are rejected under 35 USC §112, first paragraph as failing to comply with the written description requirement.

Response To Rejections Under 35 USC 112, First Paragraph

Applicants has amended claims 1, 6, 13, 24, 25 and 26 to address the rejections under the fist paragraph of Section 112, as set forth at paragraph 6, page 3, of the outstanding office action. In particular, each of the independent claims now clearly evidences that the verification method, receipt generation method, method for providing ownership of a receipt, verification device, receipt generating device and device for proving ownership of a receipt include the use of fist and second private-public signature key pairs, and that issuers that issue messages or receipts do so using the respective private signature key. As such, claims 1, 6, 13 and 24-26 are believed to comply with 35 USC §112, first paragraph, as well as claims 2-5, 23 and 30, which depend from claim 1, claims 7-12, 27 and 31, which depend from claim 6, claims 14-22, 28 and 32, which depend from claim 13, claim 33 which depends from 24, 34 which depends from 25 and 35 which depends from 35. Accordingly, applicant respectfully requests withdrawal of the first paragraph rejection of each of those pending claims.

Response To Rejections Under 35 USC 103

As mentioned above, each of claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35 were rejected under 35 U.S.C. 103 as being unpatentable over U.S. Patent 6,233, 565 to Lewis, et al. (Lewis), in view of U.S. Patent 6,976,162 to Ellison, et al. (Ellison), and further in view of U.S. Patent 5,604,805 to Brands. And claims 1-5, 12, 14-16, 18, 23, 24, 30 and 33

were rejected under 35 USC 103 as unpatentable over Lewis in view of U.S. Patent 5,850,442 to Muftic, further in view of Ellison, and still further in view of Brands.

Applicants respectfully submit that, for the reasons discussed below, Claims 1-28 and 30-35 patentably distinguish over the prior art and are allowable. None of the cited references, whether taken alone or in some combination with Lewis, disclose or suggest obtaining and verifying authenticity of a receipt using two different public-private signature key pairs, and in the manner described. The Examiner is, accordingly, respectfully asked to reconsider and to withdraw the above-identified rejections of claims 1-28 and 30-35 under 35 U.S.C. 103 by the Lewis/Ellison/Brands combination, or the Lewis/Muftic/Ellison/Bramds combination, and to allow these claims.

As explained in detail in the specification, the invention provides for issuing and verifying ownership of electronic receipts while maintaining the owner of the receipt anonymous or pseudonymous. In one aspect of the invention, a message is received by a sender that was electronically signed by the sender using a first private-public key pair. The message includes a receipt electronically signed by an issuer using a second private-public key pair. The issuer issues the receipt using the second private-public signature key pair. This receipt is sent to a holder, which might be, but is not necessarily, the owner, using a second private-public key pair. The second pair of public/private signature keys is used to verify ownership of the receipt, where the receipt is signed using this second private signature key, and then sent. Verification by decryption is carried out by a receiver of the receipt using the second public signature key, which verifies ownership of the receipt if the receiver is the owner.

The use of the two pairs of public/private signature key pairs allows the receipt to be issued and verified, while maintaining the owner of the receipt pseudonymous or anonymous. The prior art does not disclose or suggest this use of two pairs of private/public signature keys in this way.

For example, Lewis, which is the primary reference relied on by the Examiner to reject the claims, describes procedures for issuing receipts over the Internet. The Lewis system includes that goods or services are purchased by a user over the Internet from a server having a receipt generation module. Special transaction software is used to manage the printing of various communications. The procedure disclosed in Lewis is relatively standard

in many respects, except that it is done using the Internet. Importantly, Lewis does not disclose any specific mechanism to keep the owner anonymous or pseudonymous. Lewis does not mention, teach or suggest using first and second private-public key pairs to practice the invention disclosed therein.

As the Examiner has recognized, there are a number of important features of the preferred embodiment of the invention that are not shown in or suggested by Lewis. In order to remedy this deficiency of Lewis as a reference, and hold the claims rejected under 35 USC 103(a), the Examiner relies on a number of additional references, including Muftic, Ellison and Brand (independent claims 1 and 24), and including Ellison and Brand (independent claims 6, 13, 25 and 26).

Ellison describes a procedure for issuing a pseudonym to protect the identity of a platform and its use. Once the platform receives this pseudonym, subsequent communications can be performed using the pseudonym to help keep the real identity of the platform anonymous. Ellison does not mention, teach or suggest using a first and a second private-public key pair to practice the invention disclosed therein.

Muftic was cited in the Office Action for its disclosure of a method and system for performing secure electronic commerce. In the Muftic method and system disclosed, procedures are used to authenticate signed messages. It is important to note that this reference is directed primarily to authentication rather than to confidentiality. Muftic does not mention, teach or suggest using first and second private-public key pairs to practice the invention disclosed therein.

Brands describes use of a restrictive blind signature protocol in combination with a testing protocol in order that certified information may be transferred in a "blinded" way, to ensure untraceability. Brands does not mention, teach or suggest using first and second private-public key pairs to practice the invention disclosed therein.

Applicant respectfully asserts therefore, that Lewis combined with Ellison and Brands, whether alone or in combination, and Lewis, combined with Muftic and Ellison and Brands, whether alone or in combination, teach how to issue and to verify ownership of a receipt while maintaining the owner anonymous or pseudonymous as set forth in applicant's inmdependent claims. More particularly, no combination of Lewis with or without Muftic, and/or Ellison, and/or Brands, whether alone or in combination, can be said to suggest using

first and second private-public signature key pairs, where a user and receipt issuer exchange information using the first private-public key pair, and the receipt issuer and owner communicate using the second private-public key pair.

As mentioned above with respect to the Section 112 rejections, claims 1, 6, 13, 24, 15 and 26, are amended hereby to describe more expressly the feature that two private/public signature key pairs are used to obtain and verify the authenticity of the receipt. Specifically, Claims 1 and 24 are amended to describe the feature that a second private signature key is used to issue the receipt. Claims 6 and 25 are amended to describe the feature that the receipt is issued, including a reference to a designated owner and details for what the receipt has been given, in response to a message from a user using a pseudonym, where that pseudonym was issued using a first private-public key pair, and that ownership is verified using a second private-public signature key pair while maintaining that owner anonymous or pseudonymous. Claims 13 and 26 are amended and describe the feature that a receipt is generated in response to receiving a message created by a pseudonym that itself was issued using a first private-public signature key pair, and the receipt issued and a reference to the designated owner of the receipt included such that the owner verifies ownership using a second private-public signature key pair while maintaining that owner anonymous or pseudonymous.

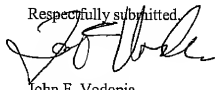
The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest the above-discussed use of two pairs of public/private signature key pairs.

This feature is of utility because, as discussed in the present application, it enables e-commerce to be transacted in a way that enables a person to verify ownership of a receipt while, at the same time, preserving that person's anonymity or psuedonymity.

Because of the above-discussed differences between claims 1, 6, 13, 24, 25 and 26, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claims 2-5, 23 and 30 are dependent from claim 1 and are allowable therewith; and claims 7-12, 27 and 31 are dependent from, and are allowable with claim 6. Similarly, claims 14-22, 28 and 32 are dependent from, and are allowable with, claim 13. Claims 33, 34 and 35 are dependent from, and are allowable with, claims 24, 25 and 26, respectively.

The amendments requested herein only emphasize or describe in more detail features already set forth in the claims. In particular, the claims 1, 6, 13, 24, 25 and 26 currently describe the use of private/public signature key pairs to issue a receipt and to verify its ownership. In view of the above discussion, the Examiner is requested to withdraw the rejections of Claims 1-28 and 30-35 under 35 U.S.C. 103, and to allow these claims. If the Examiner believes that a telephone conference with applicant's attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,



John F. Vodopia
Registration No. 36,299
Attorney for Applicant

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343
JFV:gc